CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being submitted *via* the USPTO EFS Filing System; Mail Stop Appeal Brief-Patents; Commissioner for Patents; P.O. Box 1450; Alexandria, VA 22313-1450.

Date: August 5, 2008 / Stacey Bussey/
Stacey Bussey

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

Applicant(s):	Bryan T. Starbuck, *et al.*	Examiner:	Djenane M. Bayard
Serial No:	10/601,741	Art Unit:	2141
Filing Date:	June 23, 2003		

Title: ADVANCED SPAM DETECTION TECHNIQUES

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

Applicants submit this brief in connection with an appeal of the above-identified patent application. Payment is being submitted via credit card in connection with the $510.00 fee for filing this Appeal Brief. In the event any additional fees may be due and/or are not covered by the credit card, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1063 [MSFTP438US].

I. Real Party in Interest (37 C.F.R. §41.37(c)(1)(i))

The real party in interest in this appeal is Microsoft Corporation, the assignee of the above-identified patent application.

II. Related Appeals and Interferences (37 C.F.R. §41.37(c)(1)(ii))

Appellants, appellants' legal representative, and/or the assignee of the above-identified application are not aware of any appeals or interferences which may be related to, will directly affect, or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims (37 C.F.R. §41.37(c)(1)(iii))

Claims 1-12, 42-52, and 73 are rejected. Claims 13-25, 27-41, 53-72, and 74-75 have been withdrawn, and claim 26 has been cancelled. The rejection of claims 1-12, 42-52, and 73 is being appealed.

IV. Status of Amendments (37 C.F.R. §41.37(c)(1)(iv))

Amendments were submitted in the Reply to Final Office Action dated January 10, 2008. The Examiner did not indicate in the Advisory Action dated June 23, 2008, whether or not the amendments were entered.

V. Summary of Claimed Subject Matter (37 C.F.R. §41.37(c)(1)(v))

A. <u>Independent Claim 1</u>

Independent claim 1 relates to a computer-implemented spam detection system having a message parsing component that identifies features relating to at least a portion of origination information of a message. (*See, e.g.*, Figure 1 and accompanying description at page 8, lines 10-20). The system also includes a feature pairing component that combines the features into useful pairs, and the features of the pairs are evaluated for consistency with respect to one another to determine if the message is spam. (*See, e.g.*, Figure 1 and accompanying description at page 8, lines 10-24).

B. Independent Claim 42

Independent claim 42 relates to a computer-implemented method that facilitates generating features for use in spam detection. The method includes receiving at least one message and parsing at least a portion of a message to generate one or more features. (*See, e.g.*, Figure 8 and accompanying description at page 18, lines 1-3). The method also includes combining at least two features into pairs, each pair of features creates at least one additional feature, the features of each pair coinciding with one another. (*See, e.g.*, Figure 8 and accompanying description at page 18, lines 3-4). The method further uses the pairs of features to train a machine learning spam filter regarding acceptable or unacceptable pairs. (*See, e.g.*, Figure 8 and accompanying description at page 18, lines 4-6). Moreover, the method detects a spam e-mail based at least in part on comparing one or more pairs of features in the e-mail to at least one pair in the machine learning spam filter. (*See, e.g.*, Figure 8 and accompanying description at page 18, lines 8-16).

C. Independent Claim 73

Independent claim 73 relates to a computer-implemented system that facilitates generating features for use in spam detection. The system comprises means for receiving at least one message as well as means for parsing at least a portion of a message to generate one or more features. (*See, e.g.*, Figure 1 and accompanying description at page 8, lines 10-15). The system also includes means for combining at least two features into pairs, the pairs are evaluated against each other for consistency and means for using the pairs of features to train a machine learning spam filter. (*See, e.g.*, Figure 1 and accompanying description at page 8, lines 15-24).

The means for limitations described above are identified as limitations subject to the provisions of 35 U.S.C. §112 ¶6. The structures corresponding to these limitations are identified with reference to the specification and drawings in the above-noted parentheticals.

VI. Grounds of Rejection to be Reviewed (37 C.F.R. §41.37(c)(1)(vi))

A. Whether claims 1-12, 42-52, and 73 stand rejected under 35 U.S.C. §101 as being allegedly directed to non-statutory subject matter.

B. Whether claims 1-8, 10-12, 42-49, 51-52, and 73 stand rejected under 35 U.S.C. §102(e) as being anticipated by Buford, *et al.* (US 2003/0041126).

C. Whether claims 9 and 50 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Buford, *et al.* in view of to Capiel (US 2003/0149733).

VII. Argument (37 C.F.R. §41.37(c)(1)(vii))

A. Rejection of Claims 1-12, 42-52, and 73 Under 35 U.S.C. §101

Claims 1-12, 42-52, and 73 stand rejected under 35 U.S.C. §101 because the claimed invention is allegedly directed to non-statutory subject matter. It is requested that this rejection be reversed for at least the following reason. The claims as amended recite patentable subject matter as they produce a useful, concrete, and tangible result.

> Because the claimed process applies the Boolean principle [abstract idea] to produce a ***useful, concrete, tangible result*** … on its face the claimed process comfortably falls within the scope of §101. *AT&T Corp. v. Excel Communications, Inc.*, 172 F.3d 1352, 1358. (Fed.Cir. 1999) (Emphasis added); See *State Street Bank & Trust Co. v. Signature Fin. Group, Inc.*, 149 F.3d 1368, 1373, 47 USPQ2d 1596, 1601 (Fed.Cir.1998). The inquiry into patentability requires an examination of the contested claims to see if the claimed subject matter, as a whole, is a disembodied mathematical concept representing nothing more than a "law of nature" or an "abstract idea," or if the mathematical concept ***has been reduced to some practical application rendering it "useful."*** *AT&T* at 1357 citing *In re Alappat*, 33 F.3d 1526, 31 1544, 31 U.S.P.Q.2D (BNA) 1545, 1557 (Fed. Cir. 1994) (Emphasis added) (holding that more than an abstract idea was claimed because the claimed invention as a whole was directed toward forming a specific machine that produced the useful, concrete, and tangible result of a smooth waveform display).

The claimed subject matter generally relates to detecting spam e-mail messages based at least in part on evaluating pairs of features in a message. In one example, the features can also be utilized to train a machine learning spam filter. The spam filter can be leveraged in determining whether messages are spam based at least in part on previous features and relationship thereof to spam messages. To this end, claim 1 recites ***the features of the pairs are evaluated for consistency with respect to one another to determine if the message is spam***. This is certainly a useful result to one receiving spam e-mails as such a determination can facilitate filtering the e-mail, reporting the e-mail, or any number of actions. Additionally, the result is a concrete one, as it is repeatable, and tangible as embodied in a computer-implemented system such to accord a real world value. Additionally, claim 42 recites similar aspects, namely ***detecting a spam e-mail based at least in part on comparing one or more pairs of features in the e-mail to at least one pair in the machine learning spam filter***. Such detection of spam e-mail is undoubtedly a useful and concrete result. Moreover, as claim 42 has been amended to recite a computer-implemented method, this provides sufficient tangibility to be patentable subject matter. Further, claim 73 recites ***means for using the pairs of features to train a machine learning spam filter***. Again, this is a useful and concrete result as such training mitigates the need to manually configure at least a portion of the filter. Moreover, as claim 73 has been amended to recite a computer-implemented system, this provides the requisite tangibility aspect to be patentable subject matter.

To the extent the Examiner might doubt the tangibility of the claims inferring that they are directed to software, being computer-implemented, in view of the recent Federal Circuit opinion in *Eolas Techs., Inc. v. Microsoft Corp.*, 399 F.3d 1325, 1338 (Fed. Cir. 2005), the court stated that software code alone constitutes patentable subject matter.

> Title 35, section 101, explains that an invention includes 'any new and useful process, machine, manufacture or composition of matter.' Without question, ***software code <u>alone</u> qualifies as an invention eligible for patenting under these categories, at least as processes.*** (emphasis added) (citations omitted).

Therefore, even if the claims were interpreted merely as software, they would constitute patentable subject matter under *Eolas*. It should be noted that the Examiner did not respond to this argument in the Advisory Action dated June 23, 2008. For at least the foregoing reasons, it is readily apparent that the claimed subject matter is patentable under 35 U.S.C. §101. Accordingly, rejection of claims 1-12, 42-52, and 73, under this section should be reversed.

B. Rejection of Claims 1-8, 10-12, 42-49, 51-52, and 73 Under 35 U.S.C. §102(e)

Claims 1-8, 10-12, 42-49, 51-52, and 73 stand rejected under 35 U.S.C. §102(e) as being anticipated by Buford, *et al*. It is respectfully requested that this rejection be reversed for at least the following reason. Buford, *et al.* fails to disclose or suggest each and every element recited in the subject claims.

> For a prior art reference to anticipate, 35 U.S.C. §102 requires that "***each and every element*** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)) (emphasis added).

As described, the subject matter as claimed relates to detecting spam e-mail messages; in particular, the features of origination information can be analyzed for consistency to evaluate the integrity of the e-mail. When an e-mail is transmitted, a variety of protocols are utilized having various headers and information relating to the origin of the e-mail; this information can be evaluated to determine validity of values (or features) throughout. For example, an IP address feature can be verified with a domain name feature of the same e-mail to discover if the domain is in the appropriate address or range of addresses. If not, inconsistency between this pair of features can indicate spam. Alternatively, for example, the inconsistency can be a result of misconfiguration of an e-mail server/client and can be populated in a trained spam filter to indicate that the inconsistency is not itself indicative of spam if desired. To this end, claim 1 recites *a message parsing component that identifies features relating to at least a portion of origination information of a message, and a feature pairing component that combines the features into useful pairs, the* ***features of the pairs are evaluated for consistency with respect to one another to <u>determine</u> if the message is spam***. Buford, *et al.* fails to disclose or suggest such claimed aspects.

Buford, *et al.* relates to reporting customer e-mail complaints for unsolicited commercial e-mails. In particular, Buford, *et al.* appears to disclose a system that receives a complaint of an unsolicited commercial e-mail by e-mail notification from the customer and breaks the e-mail into a plurality of headers and bodies. Typically, the innermost header is evaluated by the system as this is likely the original unsolicited e-mail. Information regarding the e-mail can be stored, such as IP address, and validated for subsequent reporting. However, Buford, *et al.* fails to disclose or suggest ***features of the pairs are evaluated for consistency with respect to one another to <u>determine</u> if the message is spam***.

On the contrary, Buford, *et al.* isolates information in messages for storage and subsequent reporting or data access. To this end, the values are input into a database, for example, such that they are isolated into cells and are, thus, not combined into pairs as recited in the subject claims. Additionally, the values of Buford, *et al.* are not evaluated to determine if a message is spam as recited in the claims; rather the message in Buford, *et al.* has already been identified as spam by the user and reported to a complaint system. Thus, no determination is made regarding spam in Buford, *et al.*, much less a determination made by evaluating the feature pairs of the e-mail with respect to one another, as recited in the subject claims.

The Examiner asserts that Buford, *et al.* teaches the same functionality as applicants' claimed subject matter as it parses e-mail messages to obtain URL, e-mail addresses, and telephone number of a spam source. (*See* Advisory Action dated June 23, 2008). Assuming *arguendo* that Buford, *et al.* does teach this, it still does not describe each and every element of applicants' claimed subject matter. For example, in addition to parsing the e-mail into features, the claims recite comparing the features to one another to determine if the message is spam. Buford, *et al.* is completely silent regarding this aspect. Furthermore, as described, the system in Buford, *et al.* already knows the message is spam (as indicated by a user) upon receiving the message for parsing whereas applicants' claims recite actually making a determination of spam based on comparison of the features. Moreover, the Buford, *et al.* system merely stores the parsed elements; no comparison ever takes place among the elements of a single e-mail in Buford, *et al.* to determine if the message is spam, as described in applicants' claims. In view of the foregoing reasons, it is readily apparent that Buford, *et al.* fails to disclose or suggest each and every element recited in claim 1.

Additionally, claim 42 recites similar aspects as well as *using the pairs of features to train a machine learning spam filter* ***regarding acceptable or unacceptable pairs, and detecting a spam e-mail based at least in part on comparing one or more pairs of features in the e-mail to at least one pair in the machine learning spam filter***. Buford, *et al.* is completely silent regarding these aspects as well. As shown *supra*, Buford, *et al.* does not disclose or suggest detecting spam e-mail; rather the e-mail has already been indicated as spam by the complainant user, and a call ticket is created and forwarded to a help desk. Moreover, Buford, *et al.* does not disclose or suggest detecting such according to comparing pairs of features of the e-mail to those of a machine learning spam filter as recited in the subject claim; rather Buford, *et al.* merely allows for reporting related to the spam e-mails. Similarly, as shown above, the Examiner's assertion regarding the teaching of Buford, *et al.*, even if taken as correct, does not arise to teaching or disclosing each and every element of claim 42 by Buford, *et al.* Accordingly, Buford, *et al.* fails to disclose or suggest each and every element as recited in claim 42.

Furthermore, Buford, *et al.* does not disclose each and every element recited in claim 73. Independent claim 73 recites similar aspects to some in claim 42, namely *means for combining at least two features into pairs, the* ***pairs are evaluated against each other for consistency*** *and* ***means for using the pairs of features to train a machine learning spam filter***. As shown above, Buford, *et al.* does not contemplate such a filter much less evaluating feature pairs against one another as recited in the subject claim.

Thus it is readily apparent that Buford, *et al.* fails to disclose or suggest each and every element recited in claims 1, 42, and 73. Thus, rejection of these claims, as well as claims 2-8, 10-12, 43-49, and 51-52, which depend therefrom, should be reversed.

C. Rejection of Claims 9 and 50 Under 35 U.S.C. §103(a)

Claims 9 and 50 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Buford, *et al.* in view of Capiel. It is respectfully requested that this rejection be reversed for at least the following reasons. Buford, *et al.* and Capiel, when taken alone or in combination, fail to teach or suggest all elements recited in the subject claims. In particular, Capiel fails to cure the aforementioned deficiencies of Buford, *et al.* with respect to claims 1 and 42, from which claims 9 and 50 depend. Accordingly, this rejection should be reversed.

F. Conclusion

For at least the above reasons, the claims currently under consideration are believed to be patentable over the cited references and recite statutory subject matter. If any additional fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFT438US].

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/David Matthew Noonan/
David Matthew Noonan
Reg. No. 59,451

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731

VIII. Claims Appendix (37 C.F.R. §41.37(c)(1)(viii))

1. A computer-implemented spam detection system comprising:

a message parsing component that identifies features relating to at least a portion of origination information of a message; and

a feature pairing component that combines the features into useful pairs, the features of the pairs are evaluated for consistency with respect to one another to determine if the message is spam.

2. The system of claim 0, each pair comprises at least one of the following:

at least one of a domain name and a host name in a MAIL FROM command;
at least one of a domain name and a host name in a HELO COMMAND;
at least one of an IP address and a subnet in a Received from header;
at least one of a domain name and a host name in a Display name;
at least one of a domain name and a host name in a Message From line; and
at least one time zone in a last Received from header.

3. The system of claim 0, the domain name is derived from the host name.

4. The system of claim 0, the subnet comprises one or more IP addresses that share a first number of bits in common.

5. The system of claim 0, a useful pair is any one of a domain name and a host name from a Message From and from a HELO command.

6. The system of claim 0, a useful pair is a Display name domain name and host name and a Message From domain name and host name.

7. The system of claim 0, a useful pair is any one of a domain name and a host name in a Message From and any one of a Received from IP address and subnet.

8. The system of claim 0, a useful pair is a sender's alleged time zone and a Message From domain name.

9. The system of claim 0, a useful pair comprises a sender's type of mailing software and any one of a domain name, host name and user name derived from one of an SMTP command and a message header.

10. The system of claim 0, origination information comprises SMTP commands, the SMTP commands comprise a HELO command, a MAIL FROM command, and a DATA command.

11. The system of claim 0, the DATA command comprises a Message From line, sender's alleged time zone, and sender's mailing software.

12. The system of claim 0, further comprising a component that applies one or more heuristics consistently to mail messages to obtain consistent feature pairing.

42. A computer-implemented method that facilitates generating features for use in spam detection comprising:

receiving at least one message;

parsing at least a portion of a message to generate one or more features;

combining at least two features into pairs, each pair of features creates at least one additional feature, the features of each pair coinciding with one another;

using the pairs of features to train a machine learning spam filter regarding acceptable or unacceptable pairs; and

detecting a spam e-mail based at least in part on comparing one or more pairs of features in the e-mail to at least one pair in the machine learning spam filter.

43. The method of claim 0, the at least a portion of the message being parsed corresponds to origination information of the message.

44. The method of claim 0, each pair comprises at least one of the following:
at least one of a domain name and a host name in a MAIL FROM command;
at least one of a domain name and a host name in a HELO COMMAND;
at least one of an IP address and a subnet in a Received from header;
at least one of a domain name and a host name in a Display name;
at least one of a domain name and a host name in a Message From line; and
at least one time zone in a last Received from header.

45. The method of claim 0, the domain name is derived from the host name.

46. The method of claim 0, the pair of features is a Display name domain name and host name and a Message From domain name and host name.

47. The method of claim 0, a useful pair is any one of a domain name and a host name from a Message From and from a HELO command.

48. The method of claim 0, the pair of features is any one of a domain name and a host name in a Message From and any one of a Received from IP address and subnet.

49. The method of claim 0, the pair of features is a sender's alleged time zone and a Message From domain name.

50. The method of claim 0, the pair of features comprises a sender's type of mailing software and any one of a domain name, host name and display name derived from one of an SMTP command and a message header.

51. The method of claim 0, further comprising selecting one or more most useful pairs of features to train the machine learning filter.

52. The method of claim 0, the detecting a spam e-mail based at least in part on one of:

receiving new messages;

generating pairs of features based on origination information in the messages;

passing the pairs of features through the machine learning filter; and

obtaining a verdict as to whether at least one pair of features indicates that the message is more likely to be spam.

73. A computer-implemented system that facilitates generating features for use in spam detection comprising:

means for receiving at least one message;

means for parsing at least a portion of a message to generate one or more features;

means for combining at least two features into pairs, the pairs are evaluated against each other for consistency; and

means for using the pairs of features to train a machine learning spam filter.

IX. Evidence Appendix (37 C.F.R. §41.37(c)(1)(ix))

None.

X. Related Proceedings Appendix (37 C.F.R. §41.37(c)(1)(x))

None.